

Lab Equipment

3.4.6 Lab – Configure VLANs and Trunking

3.5 Dynamic Trunking Protocol

3.5.1 Introduction to DTP

Some Cisco switches have a proprietary protocol that lets them automatically negotiate trunking with a neighboring device. This protocol is called Dynamic Trunking Protocol (DTP). DTP can speed up the configuration process for a network administrator. Ethernet trunk interfaces support different trunking modes. An interface can be set to trunking or nontrunking, or to negotiate trunking with the neighbor interface. Trunk negotiation is managed by DTP, which operates on a point-to-point basis only, between network devices.

DTP is a Cisco proprietary protocol that is automatically enabled on Catalyst 2960 and Catalyst 3650 Series switches. DTP manages trunk negotiation only if the port on the neighbor switch is configured in a trunk mode that supports DTP. Switches from other vendors do not support DTP.

Caution: Some internetworking devices might forward DTP frames improperly, which can cause misconfigurations. To avoid this, turn off DTP on Cisco switch interfaces that are connected to devices that do not support DTP.

The default DTP configuration for Cisco Catalyst 2960 and 3650 switches is dynamic auto.

To enable trunking from a Cisco switch to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration mode commands. This causes the interface to become a trunk, but it will not generate DTP frames.

```
S1(config-if)# switchport mode trunk
S1(config-if)# switchport nonegotiate
```

To re-enable dynamic trunking protocol use the `switchport mode dynamic auto` command.

```
S1(config-if)# switchport mode dynamic auto
```

If the ports connecting two switches are configured to ignore all DTP advertisements with the **switchport mode trunk** and the **switchport nonegotiate** commands, the ports will stay in trunk port mode. If the connecting ports are set to dynamic auto, they will not negotiate a trunk and will stay in the access mode state, creating an inactive trunk link.

When configuring a port to be in trunk mode, use the **switchport mode trunk** command. Then there is no ambiguity about which state the trunk is in; it is always on.

3.5.2 Negotiated Interface Modes

The `switchport mode` command has additional options for negotiating the interface mode. The full command syntax is the following:

```
Switch(config)# switchport mode { access | dynamic { auto | desirable } | trunk }
```

The options are described in the table.

Option	Description
access	Puts the interface (access port) into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface, regardless of whether the neighboring interface is a trunk interface.
dynamic auto	Makes the interface able to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk or desirable mode. The default switchport mode for all Ethernet interfaces is dynamic auto.
dynamic desirable	Makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or dynamic auto mode.
trunk	Puts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link. The interface becomes a trunk interface even if the neighboring interface is not a trunk interface.

Use the **switchport nonegotiate** interface configuration command to stop DTP negotiation. The switch does not engage in DTP negotiation on this interface. You can use this command only when the interface switchport mode is **access** or **trunk**. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.

3.5.3 Results of a DTP Configuration

The table illustrates the results of the DTP configuration options on opposite ends of a trunk link connected to Catalyst 2960 switch ports. Best practice is to configure trunk links statically whenever possible.

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited connectivity
Access	Access	Access	Limited connectivity	Access

3.5.4 Verify DTP Mode

The default DTP mode is dependent on the Cisco IOS Software version and on the platform. To determine the current DTP mode, issue the `show dtp interface` command as shown in the output.

```
S1# show dtp interface fa0/1
DTP information for FastEthernet0/1:
TOS/TAS/TNS: ACCESS/AUTO/ACCESS
TOT/TAT/TNT: NATIVE/NEGOTIATE/NATIVE
Neighbor address 1: C80084AEF101
Neighbor address 2: 000000000000
Hello timer expiration (sec/state): 11/RUNNING
Access timer expiration (sec/state): never/STOPPED
Negotiation timer expiration (sec/state): never/STOPPED
Multidrop timer expiration (sec/state): never/STOPPED
FSM state: S2:ACCESS
# times multi & trunk 0
Enabled: yes
In STP: no
```

Note: A general best practice is to set the interface to **trunk** and **nonegotiate** when a trunk link is required. On links where trunking is not intended, DTP should be turned off.

3.5.5 Packet Tracer – Configure DTP

In this Packet Tracer activity, you will configure and verify DTP.

3.5.5 Packet Tracer – Configure DTP

3.6 Module Practice and Quiz

3.6.1 Packet Tracer – Implement VLANs and Trunking

In this Packet Tracer activity, you will perform the following:

- Configure VLANs
- Assign Ports to VLANs
- Configure Static Trunking
- Configure Dynamic Trunking

3.6.1 Packet Tracer – Implement VLANs and Trunking

3.6.2 Lab – Implement VLANs and Trunking

In this lab, you will perform the following:

- Build the Network and Configure Basic Device Settings
- Create VLANs and Assign Switch Ports
- Configure an 802.1Q Trunk between the Switches

3.6.2 Lab – Implement VLANs and Trunking

3.6.3 What did I learn in this module?

Overview of VLANs

Virtual LANs (VLANs) are a group of devices that can communicate as if each device was attached to the same cable. VLANs are based on logical instead of physical connections. Administrators use VLANs to segment networks based on factors such as function, team, or application. Each VLAN is considered a separate logical network. Any switch port can belong to a VLAN. A VLAN creates a logical broadcast domain that can span multiple physical LAN segments. VLANs improve network performance by separating large broadcast domains into smaller ones. Each VLAN in a switched network corresponds to an IP network; therefore, VLAN design must use a hierarchical network-addressing scheme. Types of VLANs include the default VLAN, data VLANs, the native VLAN, management VLANs, and voice VLANs.

VLANs in a Multi-Switched Environment

A VLAN trunk does not belong to a specific VLAN. It is a conduit for multiple VLANs between switches and routers. A VLAN trunk is a point-to-point link between two network devices that carries more than one VLAN. A VLAN trunk extends VLANs across an entire network. When VLANs are implemented on a switch, the transmission of unicast, multicast, and broadcast traffic from a host in a particular VLAN are restricted to the devices that are in that VLAN. VLAN tag fields include the type, user priority, CFI and VID. Some devices add a VLAN tag to native VLAN traffic. If an 802.1Q trunk port receives a tagged frame with the VID that is the same as the native VLAN, it drops the frame. A separate voice VLAN is required to support VoIP. QoS and security policies can be applied to voice traffic. Voice VLAN traffic must be tagged with an appropriate Layer 2 CoS priority value.

VLAN Configuration

Different Cisco Catalyst switches support various numbers of VLANs including normal range VLANs and extended range VLANs. When configuring normal range VLANs, the configuration details are stored in flash memory on the switch in a file called `vlan.dat`. Although it is not required, it is good practice to save running configuration changes to the startup configuration. After creating a VLAN, the next step is to assign ports to the VLAN. There are several commands for defining a port to be an access port and assigning it to a VLAN. VLANs are configured on the switch port and not on the end device. An access port can belong to only one data VLAN at a time. However, a port can also be associated to a voice VLAN. For example, a port connected to an IP phone and an end device would be associated with two VLANs: one for voice and one for data. After a VLAN is configured, VLAN configurations can be validated using Cisco IOS **show** commands. If the switch access port has been incorrectly assigned to a VLAN, then simply re-enter the **switchport access vlan *vlan-id*** interface configuration command with the correct VLAN ID. The **no vlan *vlan-id*** global configuration mode command is used to remove a VLAN from the switch `vlan.dat` file.

VLAN Trunks

A VLAN trunk is an OSI Layer 2 link between two switches that carries traffic for all VLANs. There are several commands to configure the interconnecting ports. To verify VLAN trunk configuration use the **show interfaces *interface-ID* switchport** command. Use the **no switchport trunk allowed vlan** and the **no switchport trunk native vlan** commands to remove the allowed VLANs and reset the native VLAN of the trunk.

Dynamic Trunking Protocol

An interface can be set to trunking or nontrunking, or to negotiate trunking with the neighbor interface. Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which operates on a point-to-point basis only, between network devices. DTP is a Cisco proprietary protocol that manages trunk negotiation only if the port on the neighbor switch is configured in a trunk mode that supports DTP. To enable trunking from a Cisco switch to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration mode commands. The **switchport mode** command has additional options for negotiating the interface mode including access, dynamic auto, dynamic desirable, and trunk. To verify the current DTP mode, issue the **show dtp interface** command.

3.6.4 Module Quiz – VLANs
